AO 106 (Rev. 04/10) Application for a Search Warrant *(Page 1)*

UNITED STATES DISTRICT COURT
for the
Northern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* ITEMS SEIZED FROM BRENDAN CHANDLER AS IDENTIFIED IN ATTACHMENT A	)	Case No. 1:18-MJ-234 (CFH)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(identify the person or describe the property to be searched and its given location):

Please see Attachment A.

located in the Northern District of New York, there is now concealed
(identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, United States Code, Section 2422(b); Title 18, United States Code §§2252 and 2252A	Use of a facility of interstate commerce to entice/induce a minor into sex, and child pornography offenses, fully described in the attached affidavit

The application is based on these facts:

Please see attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days): Click here to enter a date. is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI TFO John F. Montesano Jr.

Printed name and title

Sworn to before me and signed in my presence.

Date: April 30, 2018

Judge's signature

City and State: Albany, NY

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

Affidavit in Support of a Search Warrant

Task Force Officer John F. Montesano Jr., being duly sworn, states as follows:

1. This affidavit is made in support of an application for a federal warrant to search (A) a Motorola phone model XT1254, seized from Brendan Chandler (the "Subject Phone"); (B) a 2015 Volkswagen Passat, license plate HKW5720, registered to Brendan Chandler (the "Subject Vehicle"); and (C) any computers, computer equipment, and/or computer or electronic media storage, cellular telephones, smart phones, digital cameras, and any digital recording devices located during the execution of the search warrant. Located within the places and persons to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations relating to the use of a facility of interstate commerce to persuade, induce, entice, and coerce, and attempt to persuade, induce, entice and coerce, an individual who has not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense, in violation of Title 18, United States Code, Section 2422(b); as well as the knowing transportation, receipt, possession and distribution of child pornography in violation of Title 18, United States Code §§2252 and 2252A (collectively, the "Subject Crimes"), as more particularly described in Attachment B.

2. Since February 2015, I have been an Investigator for the New York State Police, assigned to the Bureau of Criminal Investigation's Computer Crime Unit based in Latham, New York. I have been a State Police Officer since September 2005. I am also a Task Force Officer with the Federal Bureau of Investigation (FBI), Albany Field Office, working with agents and other officers to identify and arrest people committing and attempting to commit child exploitation offenses in violation of federal and state law.

3. In my capacity as an Investigator/Trooper I have been involved in the investigation of offenses relating to computers and the Internet, as well as investigations involving the

distribution of child pornography via the Internet, for approximately 5 years. I have received training on the subjects of online criminal investigations, the distribution of child pornography, and computer evidence handling and forensics. During my employment, I have attended trainings from the National White Collar Crimes Center (NW3C) in basic Internet investigative techniques as they apply to child pornography investigations and computer crimes. Investigators with the Internet Crimes Against Children Task Force have instructed me in techniques of child pornography and child exploitation investigations. I have successfully completed training by the National White Collar Crime Center in cyber-investigations, basic data recovery, and acquisitions and intermediate data recovery. I have also completed forensic examiner training and well as Cellebrite training. I have also successfully completed undercover chat training in Latham, New York.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the Subject Crimes are presently located within the places to be searched described in Attachment A. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

Basis for a Probable Cause Finding

5. Brendan Chandler ("Chandler"), age 34 of Glenville, New York, was arrested on April 17, 2018 and charged the following day, by criminal complaint, with a violation of Title 18, United States Code, Section 2422(b). Chandler is alleged to have used a phone and the Internet to solicit sex from someone whom he believed was a 14-year-old girl. The complaint is incorporated herein by reference and attached as an exhibit to this affidavit.

6. The Subject Phone was seized from Chandler incident to his arrest, and is in the possession of the FBI Albany Field Office. Because Chandler was arrested, the Subject Vehicle was towed out of the Walmart parking lot; it is in the control of the New York State Police, and within the Northern District of New York.

7. There is probable cause to conclude that the Subject Phone will contain evidence of violations of Title 18, United States Code, Section 2422(b). This is the only phone that Chandler possessed at the time of his arrest. This phone must necessarily be the phone he used to communicate with rachaelcheer3, because he was communicating with her as he drove into the Walmart parking lot in an attempt to meet her. There is also probable cause to conclude that the Subject Vehicle will contain evidence of violations of Title 18, United States Code, Section 2422(b). For instance, in my training and experience, an adult attempting to meet a minor for sex may possess, in their car, items that they may use and attempt to use in the course of enticing and inducing the minor into sex, including but not limited to condoms, lubrication, alcohol, controlled substances, sex paraphernalia, pornography, erotica, and gifts/money to be given to the minor. In this case, for instance, rachaelcheer3 asked Chandler to bring condoms with him. The Subject Vehicle, and electronic devices found within it, may contain other evidence of the perpetrator's intent to follow through with the plan to have sex with a minor, including driving directions and documentation of motel/hotel reservations.

8. Based on my training and experience, an adult attempting to meet a minor for sex is also likely to possess or otherwise be involved with child pornography. Based on my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides, and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are valued highly and often maintained for years and are kept close by, usually at the collector's residence, on the collector's person or in the collector's vehicle to enable the collector to view the collection at a moment's notice.

d. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, address, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Electronic Devices and Digital Storage

9. As described above and in Attachment B, this application seeks permission to search and seize records in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive or other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

10. I submit that if a computer or storage medium is found on during the execution of the search warrant, there is probable cause to believe those records will be stored in that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of

operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

11. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer, smart phone, and digital recording device (cameras) storage media can contain other forms of electronic evidence as well:

a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when, is, as described further in Attachment B, called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in *Attachment B* also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's

knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner. Also, the presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's intent. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present, and, if so, whether the presence of that malicious software might explain the presence of other things found on the storage medium. I mention the possible existence of malicious software as a theoretical possibility, only; I will not know, until a forensic analysis is conducted, whether malicious software is present in this case.

12. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. It is possible that the storage media located on the premises will contain files and information that are not called for by the warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the warrant are immediately apparent. In most cases, however, such techniques may not yield the evidence described in the warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including

electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

Conclusion

13. I respectfully request that the proposed warrant be issued authorizing the search of (A) a Motorola phone model XT1254, seized from Brendan Chandler (the "Subject Phone"); (B) a 2015 Volkswagen Passat, license plate HKW5720, registered to Brendan Chandler (the "Subject Vehicle"); and (C) any computers, computer equipment, and/or computer or electronic media storage, cellular telephones, smart phones, digital cameras, and any digital recording devices located during the execution of the search warrant, for evidence, fruits, and instrumentalities relating to the Subject Crimes, as more particularly described in Attachment B.

John F. Montesano Jr.
Task Force Officer
Federal Bureau of Investigation

SUBSCRIBED TO AND SWORN BEFORE ME
THIS 30th DAY OF APRIL, 2018

Hon. Christian F. Hummel
United States Magistrate Judge

ATTACHMENT A

PLACE AND ITEMS TO BE SEARCHED AND SEIZED

(A) a Motorola phone model XT1254, seized from Brendan Chandler (the "Subject Phone"); (B) a 2015 Volkswagen Passat, license plate HKW5720, registered to Brendan Chandler (the "Subject Vehicle"); and (C) any computers, computer equipment, and/or computer or electronic media storage, cellular telephones, smart phones, digital cameras, and any digital recording devices located during the execution of the search warrant. Both the Subject Phone and Subject Vehicle are within the Northern District of New York.

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Items and information evidencing violations of Title 18, United States Code, Section 2422(b) (enticement of a minor), and Title 18, United States Code, Sections 2252 and 2252A (distributing, receiving, transporting or possessing child pornography), specifically:

Materials Relating to Enticement of Minors

1. Items that may be used or attempted to be used in the course of enticing and inducing a minor into sex, including but not limited to condoms, lubrication, alcohol, controlled substances, sex paraphernalia, pornography, erotica and gifts/money to be given to the minor.

2. Any and all information related to or contained within the Kik Messenger application, and its use.

Materials Relating to Child Erotica and Depictions of Minors

3. Any and all visual depictions of minors, including, but not limited to sexually explicit images of minors.

4. Any and all address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

5. Any and all notebooks and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

6. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes.

Computers and Electronic Media

7. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.

8. Computer and electronic hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer and electronic hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives, secure digital (sd) cards, and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); digital cameras; cellular telephones and related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices), specifically including any cellular telephones; and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

9. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers,

interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

10. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

11. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

12. Any computer or electronic records, documents, and materials referencing relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

13. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

14. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer- related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, USB drives, secure digitial (sd) cards, or other memory storage devices.

Documents, Computer, and Internet Records

15. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, notes, and reference materials.

16. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

17. Records of address or identifying information for the target(s) of the investigation, and any email addresses, user IDs, eIDs (electronic ID numbers), and passwords.

18. Documents and records, including, for example, receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the residence and/or possession of the searched items located therein.

19. Computer records and evidence identifying who the particular user was who distributed, transmitted, downloaded or possessed any child pornography found on any computer or computer media (evidence of attribution).

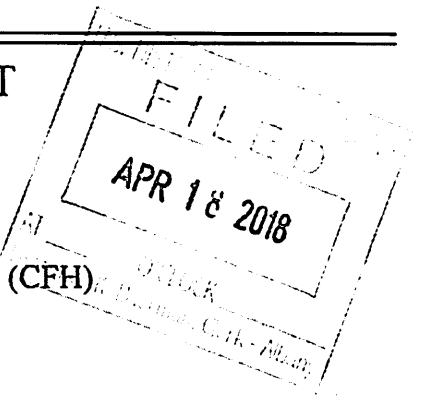
(Exhibit – April 18, 2018 Complaint Against Brendan Chandler)

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York



UNITED STATES OF AMERICA
v.

BRENDAN CHANDLER,

Defendant.

Case No. 18-MJ- 198 (CFH)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On the date of April 17, 2018, in the counties of Albany and Schenectady in the Northern District of New York, the defendant violated:

Code Section	*Offense Description*
Title 18, United States Code, Section 2422(b)	Using a facility of interstate commerce to persuade, induce, entice, and coerce, and attempt to persuade, induce, entice and coerce, an individual who has not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense under New York State law

This criminal complaint is based on these facts:
Please see attached affidavit.

☒ Continued on the attached sheet.

Attested to by the Applicant in Accordance with the Requirements of Rule 4.1 of the Federal Rules of Criminal Procedure.

Complainant's signature

FBI Task Force Officer John F. Montesano Jr.

Printed name and title

Sworn to before me and signed in my presence.

Date: April 18, 2018

Judge's signature

City and State: Albany, NY

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

Affidavit in Support of a Criminal Complaint

I, John F. Montesano Jr., having been first duly sworn, do hereby depose and state as follows:

1. I respectfully make this affidavit in support of a criminal complaint charging BRENDAN CHANDLER ("Chandler"), age 34, of Glenville, New York, with using a facility of interstate commerce to persuade, induce, entice, and coerce, and attempt to persuade, induce, entice and coerce, an individual who has not attained the age of 18 years to engage in sexual activity for which any person can be charged with a criminal offense, in violation of Title 18, United States Code, Section 2422(b).

2. Since February 2015, I have been an Investigator for the New York State Police, assigned to the Bureau of Criminal Investigation's Computer Crime Unit based in Latham, New York. I have been a State Police Officer since September 2005. I am also a Task Force Officer with the Federal Bureau of Investigation (FBI), Albany Field Office, working with agents and other officers to identify and arrest people committing and attempting to commit child exploitation offenses in violation of federal and state law.

3. In my capacity as an Investigator/Trooper I have been involved in the investigation of offenses relating to computers and the Internet, as well as investigations involving the distribution of child pornography via the Internet, for approximately 5 years. I have received training on the subjects of online criminal investigations, the distribution of child pornography, and computer evidence handling and forensics. During my employment, I have attended trainings from the National White Collar Crimes Center (NW3C) in basic Internet investigative techniques as they apply to child pornography investigations and computer crimes. Investigators with the Internet Crimes Against Children Task Force have instructed me in techniques of child pornography and child exploitation investigations. I have successfully

completed training by the National White Collar Crime Center in cyber-investigations, basic data recovery, and acquisitions and intermediate data recovery. I have also completed forensic examiner training and well as Cellebrite training. I have also successfully completed undercover chat training in Latham, New York.

4. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). As a Task Force Officer, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors, specifically those involving the exploitation of a minor for sexual purposes in violation of Title 18, United States Code, Sections 2251(a) and 2422(b).

5. The statements contained in this affidavit are based upon my investigation, information provided by other members of the State Police and the FBI's Child Exploitation Task Force, and on my experience and training as a police officer and investigator. As this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation, nor each text message that Chandler sent to an undercover online profile I maintain (discussed below). I have set forth only the facts that I believe are necessary to establish probable cause to believe that Chandler has violated Title 18, United States Code, Section 2422(b).

Basis for a Probable Cause Finding

6. Based on my training and experience, I know Kik Messenger, commonly known as Kik, to be an Internet-based messaging application. Kik allows for direct messaging between

two (2) or more people, and also allows for users to join chat groups that are organized by, among other things, geographic region and interests.

7. As part of my investigative duties, I maintained an undercover profile on Kik named "Rachaelcheer3." The profile bears a photograph of a young-looking female, pictured only from the chest down. While the picture is of an actual adult, the profile does not specify an age, or otherwise represent that the user is not a minor. I use the profile to join Kik chat groups of various titles. The titles for these groups typically mention a geographic location within Upstate New York, and do not refer directly to sex or minors.

8. On April 17, 2018, at approximately 9:03 a.m., a person with the profile name of "Brendan Chandler," and screen name "bchandler420" – which, as discussed below, was the defendant, Brendan Chandler, 34, of Glenville – directly messaged me through Kik. I believe this person found my profile through one of the chat groups I joined, though I am not sure which one. I did not do anything to initiate the conversation. All communications with Chandler were between me and him only.

9. At 9:03 a.m. on April 17, Chandler wrote to my profile: "Hey you." At 9:24 a.m., I wrote back, "Hey ….asl?"[1] which is shorthand for age, sex and location. He immediately wrote back "What's up? 24.m ny" which I understood to mean 24 years old, male and in New York. He then wrote: "You." I responded "Nm …14…f…latham ny" meaning nothing much going on, and that I was 14 years old, female and in Latham. Chandler responded that he was in Latham as well.

---

1 Misspellings, grammatical errors and abbreviations are as in the original text.

10. I told Chandler that I was in school, and specifically a private school. Chandler wrote, "That's cool. Id say I'd love to see but you are young lol." I responded "Haha .. it's kool ... if you don't wanna talk it's fine." Chandler responded "I don't mind lol. Dont get me in trouble." I responded "I won't .... Haha..." Chandler then wrote, "Send me pics." In response I sent him a photo of a young-looking adult woman from the mouth area down, wearing a tank top and shorts. I then told Chandler that I was "[i]n study hall now ..."

11. Chandler then engaged in the following conversation with my undercover profile Rachaelcheer3:

Chandler	U a virgin?
Undercover (Rachaelcheer3)	No
Chandler	How many times?
Undercover (Rachaelcheer3)	Like 3...
Chandler	Thats sexy U horny now
Undercover (Rachaelcheer3)	Haha ...no.. Lol
Chandler	U think you can handle a big dick?
Undercover (Rachaelcheer3)	Idk [I don't know]... Only seen 1 ... Lol

Chandler then sent a photograph of an erect penis. He then sent two (2) photographs depicting the naked chest of an adult male, and then wrote "Wanna try it?"

12. Chandler and my undercover profile Rachaelcheer3 then had the following conversation:

Undercover (Rachaelcheer3)	Try what ??
Chandler	Riding it
Undercover (Rachaelcheer3)	Haha .. Idk [I don't know].. Only did it wish [with] my ex
Chandler	I want you to suck it or play with it as I finger you. Then I want to lick you.
Undercover (Rachaelcheer3)	I'm only 14 .. don't u think ur too old 4 me?
Chandler	Up to you
Undercover (Rachaelcheer3)	I dk [don't know]..thats why I'm asking u .. Lol

Chandler then sent another photo of an erect penis, and then wrote "I'd eat you out and please you. As long as you don't get me in trouble lol."

13. After several more messages, including two (2) photos I sent him of a fully clothed, young woman sitting in front of lockers (but no face shown), Chandler wrote "Wyd after school?" meaning what are you doing after school? He then sent to Rachaelcheer3 a picture of a fully clothed adult male seated at the steering wheel of a car. The male in the picture appears to be the same male pictured on the driver's license issued by the New York Department of Motor Vehicles to Chandler. It is also the same person we arrested on April 17 (see below).

14. Chandler and my undercover profile Rachaelcheer3 then had the following conversation:

Chandler	I want to meet with you. Kiss. Finger you. Eat you out. Then we fuck after you suck my dick.
Chandler	Yes you can
Undercover (Rachaelcheer3)	So can u tell me what u wanna do…bc ur a lot older then me and I'll be nervous.
Undercover (Rachaelcheer3)	If I know ahead of time it would be better…lol
Chandler	Show me where you want it
Chandler	Lol

15. Chandler stated that he wanted to see Rachaelcheer3 later and that "I told you what I want to do." I asked where and stated that I was 14 years old and could not drive. Chandler stated that he would pick up Rachaelcheer3 in a car. He asked "U wanna fuck?" and Rachaelcheer3 responded "If u think I can I will … R u doing [going] to bring condoms …bc [because] I don't wanna get prego [pregnant]."

16. While assuming an identity of Rachaelcheer3, I agreed to meet Chandler in the vicinity of a Walmart in Albany County, New York, at 4:30 p.m. on April 17. Chandler's communication continued to be sexual throughout the entire time I texted with him.

17. Chandler arrived, alone, at the Walmart around 4:35 p.m. on April 17 and was arrested shortly thereafter, while pulling up (in his car) to a young woman (a plainclothed State Police Officer) that, based on the circumstances, I believe he thought was Rachaelcheer3.

18. Following his arrest, Chandler was provided his *Miranda* rights and chose to talk to law enforcement. He admitted to messaging Rachaelcheer3 and driving to Walmart to meet for the purposes of engaging in oral sex in his car with someone he thought was 14 years old. Chandler stated that he knew what he was doing was illegal and wrong, and that he was sorry for his actions.

19. The acts Chandler described that he intended to engage in with the person whom he believed to be a 14-year-old girl, as set forth above, would constitute, among others, the following crimes under New York State Penal Law:

A. New York State Penal Law § 130.30, rape in the second degree;

B. New York State Penal Law § 130.45, criminal sex act in the second degree; and

C. New York State Penal Law § 130.55, sexual abuse in the third degree.

Conclusion

20. Based on the above information, I believe that probable cause exists that BRENDAN CHANDLER has violated Title 18, United States Code, Section 2422(b), which prohibits any person from using a facility of interstate commerce to persuade, induce, entice, and coerce, and attempt to persuade, induce, entice, and coerce, an individual who has not attained the age of 18 years, to engage in sexual activity for which any person can be charged with a criminal offense. I respectfully request that a criminal complaint be issued pursuant to this violation of federal law.

John F. Montesano Jr.
Task Force Officer
Federal Bureau of Investigation

Sworn to me this 18th day of April, 2018.

Hon. Christian F. Hummel
United States Magistrate Judge